Group Theory: A Primer (CDT-11)

Luciano da Fontoura Costa
luciano@ifsc.usp.br

São Carlos Institute of Physics – DFCM/USP

June 30, 2019

Abstract

Group theory, through abstraction, provides an ample perspective on several important problems in physics, engineering, chemistry, and even music, to mention but a few areas. In this text, we provide a brief and relatively informal and non-comprehensive first view of some of the main basic concepts underlying group theory. Several of the pre-requisite concepts, such as functions and permutations, are provided before the basis of group theory is discussed, including subgroups, group homomorphisms, group action, permutation products, and permutation groups, up to Cayley's Theorem. Illustrations and examples are used as subsidies for the presentation.

'Sê plural como o universo!'

Fernando Pessoa.

1 Introduction

A great deal of the power of mathematics stems out from its *abstraction* and *generalization*. As a very simple example, the concept of a *set* and respective operations can be applied to virtually every type of elements.

Mathematical structures such as sets, vector spaces, and groups are particulalry interesting because they have intrinsic properties that are important from both theoretical and practical purposes. For instance, vectors in a vector space are closed with respect to vector addition and scalar multiplication, in the sense that these operations produce vectors that are part of the same space. So, we can be confident that applying these operations will not produce unexpected results. Vector spaces also possess many other features providing structure to them, such as vector addition associativity and commutativity, existence of addition inverse, etc.

Interestingly, mathematical structures that have more structure tend, at the same time, to become more restricted, in the sense that fewer situations will comply with the additionally imposed requirements.

Groups are mathematical structures with fewer properties than vector spaces, therefore being more general. More specifically, group theory deals with binary operations (or compositions) on a given finite or infinite set G. The required properties include closeness of the binary operation, associativity, existence of an identity element, and an inverse for every element of G.

Group theory represents one particularly interesting area of mathematics, related to abstract algebra. Lagrange was one of the first to work on related concepts, followed by other noticeable mathematicians such as Galois and Cauchy. A good deal of these initial developments focused on permutation groups as related to the solution of polynomial equations with order larger than 4.

Groups have also been the subject of interest from the *geometrical* point of view, especially symmetry groups and Lie groups, which were developed by Klein and Lie, respectively.

Nowadays, group theory is in a well-developed state, with a large number of interesting results, finding applications in a variety of areas and problems, including but not limited to Galois theory, number theory, combinatorics, chemistry, statistical physics, signal processing, pattern recognition, materials science, cryptography and music theory.

The present work is aimed at providing a very initial contact with group theory to those potentially interested in studying and applying group theory.

Some of the main basic concepts – including functions, bijection, permutations, cycles, binary operations, groups, subgroups, homomorphisms, symmetric and permutation groups, group action, Cayley theorem and stabilizers and orbits – are briefly presented in am informal and hopefully accessible way, with help of graphical respective illustrations and examples.

It should be observed that some alternative notations are sometimes used in group theory, such as the identification of groups as corresponding to the set G instead of to the tuple $(G, \circ)$. A few specific notations have also been used in the current work.

The adopted treatment is relatively informal and incomplete, so that those seeking a fully formal approach to groups should consider complementing the material in this text with other more complete and formalized material (e.g. [1, 2, 3, 4, 5, 6, 7, 8]).

2 Functions

Let A and B be two generic (finite or infinite) sets. For instance,

$$A = \{1, 3, 8, 9\} \qquad\qquad B = \{a, c, f\}$$

A *function* (or map, application) is a rule that associates a single element $f(x)$ of B to each element x in A or, more formally

$$f : x \in A \longmapsto y = f(x) \in B \tag{1}$$

The result $f(x)$ is said to be the *image* of the element x, A is commonly called the *domain* of f, and the set of all possible $y = f(x)$ is the *image* of A under f, which we will abbreviate as $I(A)$. The set B is called the *codomain* of f, with $I(A) \subset B$. Observe that there is nothing in the adopted definition that would not allow us to take $B = A$.

For instance, in the case of the previous set we could have

$$f(1) = c; \quad f(3) = a; \quad f(8) = a; \quad f(9) = c$$

Some functions (e.g. on a finite set G of N elements) can be represented by using *Cauchty's* two-line notation, which consists of using a matrix with 2 lines and N columns, each one corresponding to each of the elements of G). In the case of the previous function, we have

$$P_1 = \left(\begin{array}{cccc} 1 & 3 & 8 & 9 \\ c & a & a & c \end{array} \right)$$

Observe that the element f of set B cannot be obtained by applying f to any of the elements of A, i.e. it does not belong to the image of A under this function, and we have that $B \neq I(A)$.

When $B = I(A)$, we say that the function is *surjective.* If each of the elements in B is the image of a unique element in A, then the function f is *injective* or *one-to-one.*

Observe that it is possible that two or more elements of A be mapped into the same element in A. On the other hand, perhaps the most important feature of functions is that they *cannot* map any of the elements $x \in A$ to more than *just one* element in B.

Functions that are both surjective and injective are particularly important and are called *bijective.* This type of function is special because it allows its *inverse* to be defined respectively as

$$f^{-1} : y \in B \longmapsto x = f^{-1}(y) \in A \tag{2}$$

for any element $y \in B$. By comparing Equations 2 and 1, we immediately conclude that f^{-1} is also a function. This type of functions are called *invertible.* Observe that $x = f^{-1}(f(x))$.

Given two functions $f : x \in A \longmapsto y = f(x) \in B$ and $g : x \in (C \supset B) \longmapsto y = f(x) \in D$, the application of f followed by g, henceforth represented as $g(f(x))$, is commonly called the *composition* of g over f. We have that $gf : x \in A \longmapsto y = g(f(x)) \in D$. Observe that, in general, $gf \neq fg$, i.e. function composition is not necessarily commutative.

Function composition gives rise to the issue whether $h(gf) = (hg)f$. When this equality holds for every input $x \in A$, we say that the composition is *associative.* iiii

Bijective mappings of the elements of A into A are particularly interesting as they correspond to *permutations* of those elements. For instance, if $A = \{a, b, c\}$, we have as a possible permutation $P(a) = b$; $P(b) = c$; and $P(c) = a$.

It can be verified that a set A with N elements (i.e. $\#A = N$) will yield $N!$ (N factorial) permutations.

Given that the order of the elements of a set is immaterial, permutations are instead commonly ex-

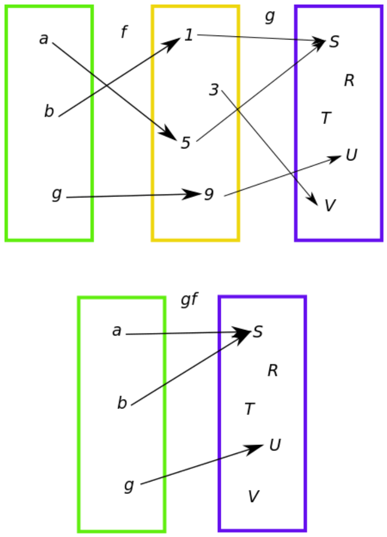


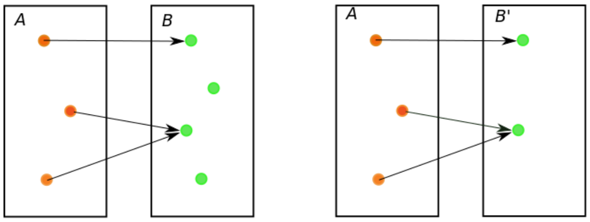
Figure 1: .

pressed as *tuples* $(a_1, a_2, \ldots, a_N)$. So, the whole possible set of permutations of $A = \{a, b, c\}$ is $\{(a, b, c,); (a, c, b); (c, a, b); (c, b, a); (b, c, a); (b, a, c)\}$.

3 A Simple Regularization Approach

Bijective functions establish a well-defined pairwise interrelationship between sets A and B. For instance, if $A = B = \mathbb{R}$ we have that the function $f(x) = x$, is invertible, while $f(x) = x^2$ is not, because it is neither injective nor surjective.

Given a function that is injective but not surjective, if we redefine its codomain as $B = I(A)$, in the sense that the elements of B that are not image of elements in A are removed, it is possible to obtain a respective inverse, as illustrated in Figure 2. This procedure is often called *restriction* of the codomain.



(a) (b)

Figure 2: A function that is not surjective (b) can become surjective by restricting the codomain set B so that only elements receiving images from A are left (b). The resulting function is $f(x \in A) \longmapsto y \in B'$.

More generally, given a generic function f that may be neither surjective nor injective, it is possible to derive at least one respective inverse f^{-1} in case we are willing to change the function to a sometimes substantial level.

A possible procedure involves two steps: (i) identify each element $y \in B$ that is image of more than one element in A, and remove all but one maps into y (according to some criterion or priority); and (ii) identify the elements of B that are not image of any element in A and remove these elements.

It is common to call the situation corresponding to non-invertible mappings as *ill-posed problems*. The above suggested procedure provides a simple means to *regularize* this situation through the application of *restrictions* on the domain and image sets, as well as on the function itself. Observe that typically there is more than one way to perform this regularizing procedure.

Let's illustrate this procedure with respect to the function $f(x) = x^2$, with $A = B = \mathbb{R}$. As we have seen, this function is neither injective nor surjective, so we start by eliminating the mappings from elements $x \in A$ such that $x < 0$, i.e. $\tilde{A} = [0, \infty)$. Observe that there could be many other choices, such as taking $\tilde{A} = (-\infty, 0]$. The function is now injective, but the set of elements $y \in (0, \infty)$ is not wholly obtainable by applying f to any of the elements of $\tilde{A}$, implying non-surjectivity. This can be avoided by making $\tilde{B} = [0, \infty)$, so that the new mapping $\tilde{f} : \tilde{A} \longmapsto \tilde{B}$ is bijective and invertible, with $\tilde{f}^{-1} = +\sqrt{\tilde{f}(x)}$.

4 Permutations

We have already observed that a function h on G that is bijective on itself is a *permutation*. Cauchy's two-line notation can be used to represent permutations. For instance, the permutation P_1 defined by $G = \{0, 1, \ldots, 11\}$ and $h(x \in G)$ being the remainder of the division of $x + 4$ by 12 (i.e. $h(x) = R(x + 4, 12)$) can be represented as the following 2×12 matrix

$$P_1 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 0 & 1 & 2 & 3 \end{pmatrix}$$

where the first row of this matrix corresponds to the elements of G in any order and the second line indicates the results of the respective application of the function h.

A *cycle* emanating from $x \in G$ is the tuple consisting of x followed by the results obtained by successive applications of h until we get back to x. For instance, in the previous example, starting with $x = 2$ we have the cycle

$$(2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,0\,1) \tag{3}$$

Observe that if $(a_1\, a_2, a_3, \ldots, a_N)$ is a cycle with length N, so will be the tuples $(a_2\, a_3, \ldots, a_N, a_1)$; $(a_3\, a_4, \ldots, a_N, a_1, a_2)$; and so on. Actually, all these cycles can be considered identical one another.

Let's consider another permutation

$$P_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 2 & 1 & 7 & 0 & 5 & 4 & 8 & 9 & 10 & 6 & 11 \end{pmatrix}$$

Starting from 0, we obtain the cycle $(0\,3\,7\,8\,9\,10\,6\,4)$. Similarly, when we start from 1, we get $(1\,2)$. For $x = 5$, it follows (5), for $x = 11$ we have (11).

An alternative way to represent permutations is to use *cycle notation*, which corresponds to the set of all possible cycles (without repetition). For instance, in the case of the previous permutation, it can be represented by the set

$$\{(0\,3\,7\,8\,9\,10\,6\,4)\,;(1\,2)\,;(5)\,;(11)\} \tag{4}$$

For simplicity's sake, cycles of length one are omitted, and the permutation is simply represented without the set notation. For instance, in the previous example we could represent the permutation as

$$(0\,3\,7\,8\,9\,10\,6\,4)\,(1\,2) \tag{5}$$

A permutation is called a *cyclic permutation* if it contains a single cycle. Permutation P_1 above is a cyclic permutation, but P_2 is not.

The *identity permutation* on $G = \{a1, a2, \ldots, a_N\}$ corresponds to

$$I = \begin{pmatrix} a_1 & a_2 & \ldots & a_N \\ a_1 & a_2 & \ldots & a_N \end{pmatrix}$$

As permutations are bijective functions, they are necessarily invertible, and the respective inverse can be obtained by exchanging the first and second rows in the Cauchy's two-line representation.

In cycle notation, the inverse permutation can be obtained by reversing the order of the representation. In the case of the previous example we have

$$[(0\,3\,7\,8\,9\,10\,6\,4)\,(1\,2)]^{-1} = (2\,1)\,(4\,6\,10\,9\,8\,7\,3\,0) \tag{6}$$

Observe that this tuple notation is not equivalent to matrix product, and neither is the -1 exponent related to matrix inversion.

5 Binary Operations, or Compositions

So far, we have seen how a function can map from elements in a set A producing images in another set B. It is possible to generalize this concept regarding relatively more ellaborate domain sets.

Let's consider the situation in which a set A is obtained from pairwise juxtapositions of elements from two sets A_1 and A_2. More formally, we consider the operation of *Cartesian product* $A_1 \times A_2$ between two sets A_1 and A_2, which is defined as corresponding to elements z such that

$$z \in (A_1 \times A_2) \iff z = (x, y) \tag{7}$$

for every $x \in A_1$ and $y \in A_2$.

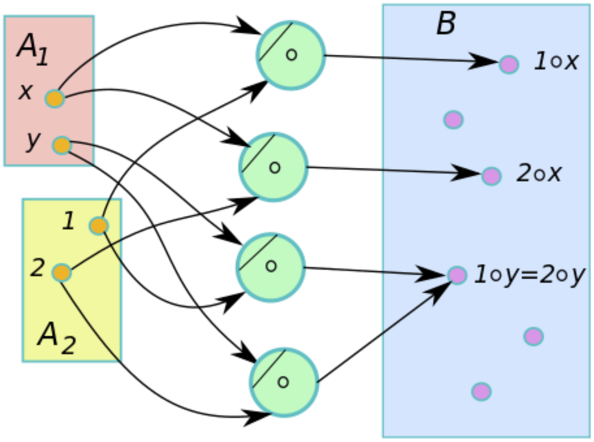


Figure 3: A binary operation $\circ$ taking values from the Cartesian product of two sets A_1 and A_2 into an image set B. Observe that this mapping needs not to be surjective or injective, and that the input channels to the binary operation are not necessarily commutative.

For instance, if $A_1 = \{1, 2\}$ and if $A_2 = \{a, b, c\}$, it follows that

$$A_1 \times A_2 = \{(1, a); (1, b); (1, c); (2, a); (2, a); (2, a)\}$$

Observe that the Cartesian product of two sets with respective sizes (or *cardinalities*) N and M will have NM elements.

Now, it is possible to extend the concept of function as acting on a domain given by a Cartesian product of set A_1 and A_2 and taking images on a set B as

$$f : (x, y) \in A_1 \times A_2 \longmapsto z = f(x, y) \in B \tag{8}$$

For instance, in the case of the previous example, and choosing $B = \{\alpha, \beta\}$, we can make

$$\begin{array}{cc} f\,(1, a) = \beta & f\,(2, a) = \alpha \\ f\,(1, b) = \beta & f\,(2, b) = \alpha \\ f\,(1, c) = \beta & f\,(2, c) = \alpha \end{array}$$

This type of functions, which are often called *binary operations* (because the act on a pair of elements) or *compositions*, provides one of the basis for defining groups. Binary operations can also be represented as $\circ(x, y) = x \circ y$ or simply xy. Observe that we cannot guarantee that $x \circ y = y \circ x$, i.e. composition is not necessarily *commutative.*

Binary operations as defined above can be represented by respective *tables.* For instance, in the case o the example above we get

	1	2
a	β	α
b	β	α
c	β	α

Henceforth, we restrict our attention to binary operations so that $A_1 = A_2 = B$, corresponding to situations where the binary combinations act on elements of a same set yielding results belonging to this same set.

For instance, in case $A_1 = A_2 = B = \mathbb{R}$, the traditional operation of addition provides an example of a commutative binary operator.

As an additional example, consider the sets $A_1 = A_2 = B = \{0, 1, 2\}$ and the operator R as corresponding to the remainder of the division of $x + y$ by 3, so that $x \in A_1$ and $y \in A_2$. We have that

$$\begin{array}{ccc} R\,(0, 0) = 0 & R\,(1, 0) = 1 & R\,(2, 0) = 2 \\ R\,(0, 1) = 1 & R\,(1, 1) = 2 & R\,(2, 1) = 0 \\ R\,(0, 2) = 2 & R\,(1, 2) = 0 & R\,(2, 2) = 1 \end{array}$$

It is interesting to observe that binary operations can be applied *recursively*, or in composition, i.e.

$$R\,(R(x, y), z) = (x \circ y) \circ z = (xy)z \tag{9}$$

or

$$R\,(x, R(y, z)) = x \circ (y \circ z) = x(yz) \tag{10}$$

Binary operations such that $(x \circ y) \circ z = x \circ (y \circ z)$ are said to be *associative.* In this case, with some abuse of notation, we can write $x \circ y \circ z$. An example of binary operation that is not commutative is the subtraction of two real numbers. For instance $1 - (2 - 3) = 2$ and $(1 - 2) - 3 = -4$.

??????

6 Groups

We are now in position to define a *group* as an ordered pair $(G, \circ)$, where G is a non-empty set endowned with a binary operation or composition $\circ$ on $G \times G \longmapsto G$, i.e. $z = y \circ x$ with $x, y, z \in G$, so that the following *group axioms* are observed:

- (a) $\circ$ is *associative*, i.e. $(z \circ y) \circ x = z \circ (y \circ x)$;

- (b) there is an *identity* (or *neutral*) element $e \in G$ so that $e \circ x = x \circ e = x$ for any $x \in G$ (in particular, $e = e \circ e$);

- (c) for any $x \in G$ there is a respective *inverse* $x^{-1} \in G$ so that $x \circ x^{-1} = x^{-1} \circ x = e$.

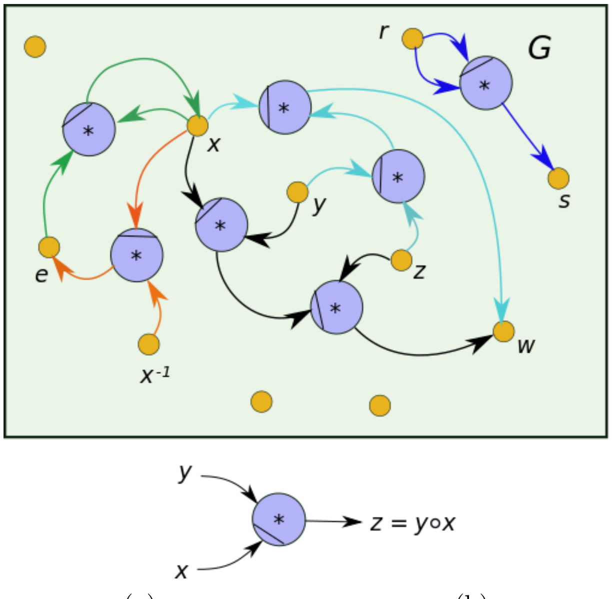
Let's suppose that $x \circ y = e$ and $z \circ x = e$. We have that $z = z \circ e = z \circ (x \circ y) = (z \circ x) \circ y = e \circ y = y$. In other works, the inverse x^{-1} is *unique*, and so is e.

In case all the above properties are verified, except the existence of the inverse (c), the tuple $(G, \circ)$ is called a *monoid.* In case (b) is also not obeyed, we still have a *semigroup.*

Figure 4 illustrates a generic group on a generic set G. The binary operators, or compositions, represented in blue, have two distinct inputs and one output. The input with a dash distinguishes the two operands in a generic binary operation $z = y \circ x$. For simplicity's sake, not every binary operation is shown.

This figure also illustrates the operation $x = x \circ e$ (in green), $s = r \circ r$ and $e = x^{-1} \circ x$ (in orange). The associative property is illustrated by the cyan, with respect to $(z \circ y) \circ x$, and black regarding $z \circ (y \circ x)$, yielding the same result w in both cases.

Observe that the binary operation is non-symmetric with respect to its input, for it is not guaranteed that



(a) (b)

Figure 4: A generic group $(G, \circ)$. The elements of G are shown in yellow, and the binary operators in blue. The identity element property is illustrated in green, and the inverse x^{-1} of and element x in orange.

$x \circ y = y \circ x$. A group $(G, \circ)$ so that $\circ$ is also commutative is called an *abelian* group. Figure 5 illustrates the fact that in an abelian group the two inputs of the respective binary operator are undistinguishable.

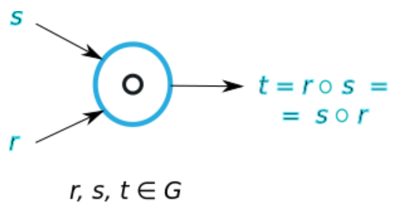


Figure 5: The two input channels of a binary operator associated to an abelian group are undistinguishable.

Let's consider another, very simple group defined in terms of $G = \{1, -1, i, -i\}$, where $i = \sqrt{-1}$, and the binary operation of complex multiplication. This binary operation $\circ$ can be represented in terms of the table

	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

where the sequence along the lines and columns are $(1, -1, i, -i)$.

Another example of group $(G, \circ)$ is defined by Integer multiplication on $\mathbb{Z}^*$ excluding the zero element (also abbreviated as $\mathbb{Z} - \{0\}$), with the identity element corresponding to 1. The exclusion of zero is because there is no inverse of the operation $0 \circ x$. Another group is the real addition, having 0 as neutral element. Both these two groups are Abelian.

Given a subset H of G (i.e. $H \subset G$) and a binary operation $\circ$, represented in terms of the tuple $g = (G, \circ)$, the H with $\circ$ will define a *subgroup* of G represented as $(H, \circ)$ if H is itself a group under the same binary operation $\circ$. The operation $\circ$ is therefore restricted to H.

The sets $gH = \{gh : g \in G, h \in H\}$ and $Hg = \{hg : g \in G, h \in H\}$ are called, respectively, the left and right *cosets* of H in G with respect to g.

7 Special Types of Groups

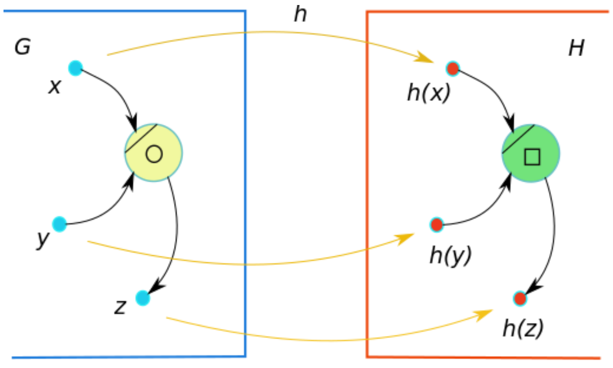
Let two groups $g = (G, \circ)$ and $h = (H, \Box)$, and consider the function $h : G \mapsto H$. If

$$x \circ y = z \iff h(x) \Box h(y) = h(z) \tag{11}$$

for any x, y, $z \in G$, we say that the function h establishes a *group homomorphism* of g into h. This means that the operation structure of G with $\circ$ is somehow preserved in H with $\Box$.

An alternative definition of group homomorphism is based on the requirement

$$h(x \circ y) = h(x) \Box h(y) \tag{12}$$



(a) (b)

Figure 6: The function h establishes a homomorphism of $g = (g, \circ)$ into $h = (H, \Box)$ iff $x \circ y = z \iff h(x) \Box h(y) = h(z)$ for any x, y, $z \in G$.

As an example of group homomorphism, consider the set I of all integers with the traditional binary operation addition, as well as the set of complex values $G = \{1, -1, i, -i\}$ with the binary operation of multiplication. The mapping $f : I \longmapsto G$ with $h(x) = i^x$ for $x \in I$ is a homomorphism because, for any $x, y \in I$ we have $h(x + y) = i^{x+y} = i^x\, i^y = h(x)\, h(y)$,

An homomorphism that is bijective is called an *isomorphism.*

A group homomorphism where $G = H$ is called an *endomorphism.*

A bijective endomorphism is an *automorphism.*

8 Permutation Products and Permutation Groups

Let's go back to the subject of permutations. If we have two permutations P and Q, defined by respective functions g and f acting on set G and taking values in G, we can compose them in the sense of applying one subsequently to the other.

Here, we understand the *permutation product* or *composition* $P \circ Q$ to correspond to the application of function Q followed by P. Observe that the result of a product permutation is also a permutation.

In Cauchy's two-line notation, the permutation product of P and Q can be obtained by juxtaposing the matrices P and Q and reorganizing the former so that its first row becomes identical to the second row of P. The resulting composition is given by the matrix having the first row as in Q and the second as in the modified version of P.

As an example, consider $G = \{0, 1, 2, 3, 4\}$ and the permutations

$$P = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 0 & 3 \end{pmatrix}; \quad Q = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 & 0 \end{pmatrix}$$

We have $P \circ Q$ given as

$$P \circ Q = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 0 & 3 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 & 0 \end{pmatrix}$$

Arranging P as indicated above yields

$$P \circ Q = \begin{pmatrix} 4 & 2 & 3 & 1 & 0 \\ 3 & 4 & 0 & 2 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 & 0 \end{pmatrix}$$

The result is

$$P \circ Q = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 2 & 1 \end{pmatrix}$$

Let S_n be the set p of all possible permutations on a set S containing n elements. Since the composition (or binary operation) $P \circ Q$ is well-defined and closed on the set S_n for any permutations P and Q, and given that there is an identity permutation I, as well as an inverse Q^{-1} for any $Q \in \Omega$ (remind that permutation products are bijective, and therefore invertible), it follows that S_n is a *symmetric group* with the binary operation, or composition $\circ$.

Subgroups of S_n are called *permutation groups.* Though these groups typically refer to $S = \{1, 2, \ldots, n\}$, here we also consider more general sets such as $S = \{a, b, \ldots\}$.

For instance, $G = \{a, b, c\}$. The set of all possible respective permutations S_3 contains the elements

$$\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}; \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}; \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix};$$
$$\begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}; \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}; \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$$

The set S_3 can also be specified in terms of its cycles, i.e. $S_3 = \{e; (bc); (ac); (ab); (acb); (abc)\}$.

An example of respectively derived permutation group is $(H, \circ)$ with

$$H = \left\{ \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}; \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} \right\} \tag{13}$$

9 Group Action on a Set

We have seen that a binary operation $\circ$ on elements of a set G take a pair of elements from this *same* set in a given order and produce as result an element that also belongs to G. This is illustrated in Figure 7(a).

In case the tuple $g = (G, \circ)$ as above obeys the group axioms, it is qualified as a group, which has an interesting structure on itself. It is often useful to consider how such a group can act on a set X other than G. More specifically, a counterpart '.' of the binary operator $\circ$ involved in g can take one element from X and one from G, yielding results in X. Figure 7(b) illustrates the resulting *left* and *right action* of g in X.

If the rule '.', obeys the following conditions, it can be said that the group *left-acts* on X, producing results x on X.

- $e.x = x$, and e is the identity element in G;

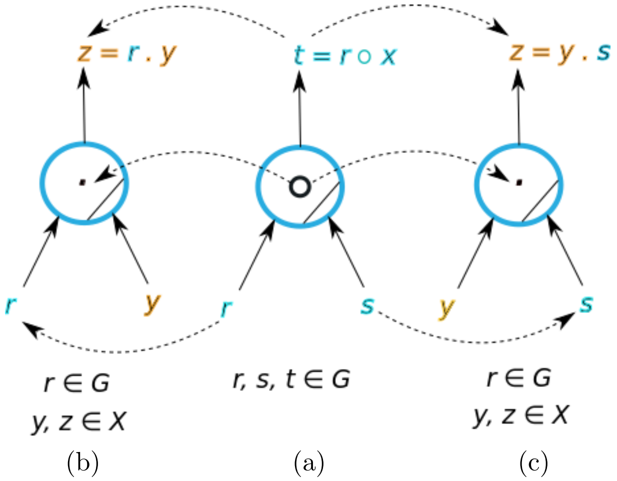


Figure 7: (a) The binary operation $\circ$ of a group $(G, \circ)$ takes elements $r, s \in G$ into an element $t \in G$. (b) This operation can be mapped into a *left action* '.' of the group on an element $y \in X$ yielding $z \in X$. (c) The *right action* on X.

- $g.(h.x) = (g.h).x$ for every $g, h \in G$.

The group *right-action* on X requires that

- $x.e = x$, and e is the identity element in G;
- $(x.g).h = x.(g.h)$ for every $g, h \in G$.

As an example, let's consider that G contains as elements

$$r = \begin{bmatrix} cos(\alpha) & -sin(\alpha) \\ sin(\alpha) & cos(\alpha) \end{bmatrix} \tag{14}$$

This set, for any $\alpha \in \mathbb{R}$, together with the binary operation '.' of matrix multiplication defines a respective rotation group $g = (G, .)$, with identity element e_G given as

$$e_G = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{15}$$

and each element r having respective inverse

$$r^{-1} = \begin{bmatrix} cos(\alpha) & sin(\alpha) \\ -sin(\alpha) & cos(\alpha) \end{bmatrix} \tag{16}$$

This group can be made to *left-act* on the set X of column vectors $\vec{v} \in \mathbb{R}^2$ through the binary operation corresponding to the product of a matrix by a column vector, i.e. $r\vec{v}$, i.e.

$$\begin{bmatrix} v'_1 \\ v'_2 \end{bmatrix} = \begin{bmatrix} cos(\alpha) & -sin(\alpha) \\ sin(\alpha) & cos(\alpha) \end{bmatrix} . \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \tag{17}$$

It can be easily verified that this formally corresponds to a left-action of g on X taking column vectors into respective column vectors *counter-clockwise* rotated by the angle α.

The right-action of G on the set Y of row vectors is given as

$$\begin{bmatrix} v'_1 & v'_2 \end{bmatrix} = \begin{bmatrix} v_1 & v_2 \end{bmatrix} . \begin{bmatrix} cos(\alpha) & -sin(\alpha) \\ sin(\alpha) & cos(\alpha) \end{bmatrix} \tag{18}$$

Observe that this action now rotates the vectors in *clockwise* direction.

Let's consider the interesting case defined by permutation groups of a set S, such as H in Equation 13. This group can act on the set $X = \{1, 2, 3\}$ by considering the respective permutation rules while taking into account the associations $1 \leftrightarrow a$; $2 \leftrightarrow b$ and $3 \leftrightarrow c$.

Cayley Theorem states that every group G is isomorphic to a subgroup of the symmetric group acting on G.

The following concepts of stabilizer and orbit are presented only with respect to left-action, as the respective right action counterparts are relatively easy to be derived.

Let $g = (G, \circ)$ be a group acting on a set X through a rule '.'. The *stabilizer* os this action with respect to $x \in X$ is the set $Stab_G(x)$ containing the elements h of G such that $h.x = x$. Observe that the identity element e_G always belong to the stabilizer set. In the case of S_3 as above, we have $Stab_{S_3}(a) = \{e; (bc)\}$.

The orbit of group g with respect to an element $x \in X$ is the set $Orb_G\{x\}$ of all elements $y \in X$ such that $y = h.x$ for some $h \in G$. If $x \in X$, then $x \in Orb_G(x)$, since $ex = x$.

In the case of the previous rotation example of group action, we have that the orbit of any vector $\vec{v} \in \mathbb{R}$ is the set of all vectors with the same magnitude as $\vec{v}$.

Recall that $Stab_G(x) \subset G$ and $Orb_G(x) \subset X$.

It is interesting to notice that the distinct orbits of a group acting on a set X provide a partitioning of that set.

10 Concluding Remarks

We have provided a concise and relatively informal very initial approach to some of the most basic concepts from group theory, up to group action, stabilizers and orbits.

The potential of group theory for studying several mathematical issues has been illustrated graphically and with respect to some simple examples. It is interesting to observe that the relatively few structural properties required from groups allow several interesting results to be obtained.

All in all, it is hoped that the presented material has motivated the potential of group theory for dealing with several diverse problems. Further insights about group concepts and applications can be obtained by probing further the related literature (e.g. [1, 2, 3, 4, 5, 6, 7, 8]).

Acknowledgments.

Luciano da F. Costa thanks CNPq (grant no. 307085/2018-0) for sponsorship. This work has benefited from FAPESP grant 15/22308-2.

References

[1] D. E. Mansfield and M. Brukheimer. *Background to Set and Group Theory.* Chatto and Windus, 1965.

[2] James S. Milne. Group theory (v3.13), 2013. Available at www.jmilne.org/math/.

[3] F. Ace-Sánchez, O. A. Agustin-Aquino, E. Lluis-Puebla, M. Montiel, and J. du Plessis. *An Introduction to Group Theory.* Venture Publishing, 2013.

[4] J. S. Rose. *A Course on Group Theory.* Dover, 1978.

[5] M Hamermesh. *Group Theory and its Application to Physical Problems.* Dover, 1962.

[6] B. Baumslag and B. Chandler. *Group Theory.* McGraw-Hill, 1968.

[7] B. Shillito. Group theory, 2013. `https://www.youtube.com/watch?v=WwndchnEDS4`. Online; accessed 30-June-2019.

[8] N. J. Wildberger. Group theory, math history, 2014. `https://www.youtube.com/watch?v=VSB8jisn9xI`. Online; accessed 30-June-2019.